#4

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Docket: 245-53434	Serial: 09/621,000
	Applicant: Tenca et al.	
	Filed: July 21, 2000	Art Unit: 2766

OTHER DOCUMENTS

M			Kaliski, Jr., B.S., "The Montgomery Inverse and Its Applications," IEEE Trans. on Computers 44:1064-1065 (August 1995)
			Montgomery, P.L., "Modular Multiplication Without Trial Division," Math. of Computation 44:519-521 (April 1985)
			Koç, Ç.K. et al., "Analyzing and Comparing Montgomery Multiplication Algorithms," IEEE Micro 16:26-33 (June 1996)
			Dhem, J. et al., "SCALPS: Smart Card For Limited Payment Systems," IEEE Micro 16:42-51 (June 1996)
			Diffie, W., Hellman, M.E., "New Directions in Cryptography," IEEE Trans. on Information Theory 22:644-654 (1976)
			Rivest, R.L. et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM 21:120-126 (1978)
			Koç, Ç.K., Acar, T., "Fast Software Exponentiation in GF(2^k)" in Proceedings, 13th Symposium on Computer Arithmetic, pp. 225-231 (July 1997) (T. Lang et al., editors)
			Hamano, T. et al., "$O(n)$-Depth Circuit Algorithm for Modular Exponentiation" in Proceedings, 12th Symposium on Computer Arithmetic, pp. 188-192 (July 1995) (S. Knowles, W.H. McAllister, editors)
M			Orup, H., "Simplifying Quotient Determination in High-radix Modular Multiplication" in Proceedings, 12th Symposium on Computer Arithmetic, pp. 193-199 (July 1995) S. Knowles, W.H. McAllister, editors)

EXAMINER:	DATE 1/15/06

*Examiner: Initial if considered, whether or not in conformance with MPEP 60; draw line through cite if not in conformance and not considered. Send copy.

#4

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Docket: 245-53434	App. 09/621,020
	Applicant: Tenca et al.	
	Filed: July 21, 2000	Art Unit: 2766

OTHER DOCUMENTS

CM			Bernal, A., Guyot, A., "Design of a Modular Multiplier Based on Montgomery's Algorithm" in 13th Conference on Design of Circuits and Integrated Systems, pp. 680-685 (November 1998)
			Eldridge, S.E., Walter, C.D., "Hardware Implementation of Montgomery's Modular Multiplication Algorithm," IEEE Trans. Computers 42:693-699 (June 1993)
			Kornerup, P., "High-Radix Modular Multiplication for Cryptosystems" in Proceedings, 11th Symposium on Computer Arithmetic, pp. 277-283 (June 1993) (E. Swartzlander et al., editors)
			Walter, C.D., "Space/Time Trade-offs for Higher Radix Modular Multiplication Using Repeated Addition," IEEE Trans. Computers 46:139-141 (1997)
			Royo, A., et al., "Design and Implementation of a Coprocessor for Cryptography Applications," European Design and Test Conference, pp. 213-217 (March 1997)
			Koç, Ç.K., Acar, T., "Montgomery Multiplication in GF(2*k*), "Designs, Codes and Cryptography 14:57-69 (1998)
CM			Tenca, A.F., "Variable Long-Precision Arithmetic (VLPA) for Reconfigurable Coprocessor Architectures," Ph.D. Thesis, University of California at Los Angeles (March 1998)

EXAMINER: CM	DATE 1/15/06

*Examiner: Initial if considered, whether or not in conformance with MPEP 60; draw line through cite if not in conformance and not considered. Send copy.